Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP04/014837

International filing date: 30 December 2004 (30.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: EP
Number: 03 029 968.9
Filing date: 30 December 2003 (30.12.2003)

Date of receipt at the International Bureau: 16 February 2005 (16.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03029968.9

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03029968.9
Demande no:

Anmeldetag:
Date of filing: 30.12.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Wibu-Systems AG
Rüppurrer Strasse 52-54
76137 Karlsruhe
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method to restore data

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F11/14

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Bemerkungen:
Remarks: See page 1 of the description for the original title
Remarques:

WIBU-SYSTEMS AG

Invention Description

WIBU-P002 - Single Action License Restore Process

Marcellus Buchheit

Version 1.00 of 22. December 2003

Confidential (Level II)

Distribution permitted only inside WIBU-SYTEMS AG, to distributors or to technical partners.
Do not send to customers or any other interested persons!

Preliminary/Under Construction

Distribution permitted inside WIBU-SYTEMS AG or to distributors, technical partners, customers or any interested persons.
The contents of this document are preliminary and subject to change.

Contents

Pages in Document: 6

List of Figures

Error! No table of figures entries found.

List of Tables

Error! No table of figures entries found.

1 Abstract

The invention describes a method to restore data, which is stored in a broken computer hardware device by transferring them partially or completely into another hardware device of same type. The stored data represents digital rights management, pay-per-use counter values or access-control tokens; in this document the word *license* is used for all these data. These licenses are created (and owned) by *different* licensors (software development companies, document authors and publishers etc.). The user as owner of the device typically buys these licenses by paying money to receive secret sequences from the different licensors, who store sequentially all licenses into the hardware. In dependence of the paid price, the sum of stored licenses represents a more or less high financial value. If the hardware device is broken or lost, these licenses cannot be longer used; without a transfer of these licenses to another hardware device, the stored financial value is lost. The method of the invention permits a restoring process of the licenses into another hardware device. This restore is based on backup data outside of the hardware device, typically in a computer data file. The license transfer is fully controlled by the licensors as owners of the specific licenses. The restore process is executed by the user via a single start operation activity ("single click"). For this a Web Service is used, which delegates the recreation of the licenses via Restoring Web Services into the new hardware device – security-specific for each license. An additional technique named as *locking* avoids that the restored (lost or broken) hardware device can be used any longer concurrently to the device with the restored licenses.

1.1 Example

An example for such a device is the CM-Stick, this is a hardware-based security and digital rights management controlling device, which is available at the USB interface.

1.2 New Features

The invention permits an easy-to-use partially or fully restoring of licenses, which are stored in a hardware device in a manner, which is fully controlled by the licensors as owners of the licenses. The reuse of the replaced hardware device is restricted.

2 The Details

2.1 How the Method Works

The complete backup mechanism is explained in the document [1]. This document here describes only the core part of the invention.

The hardware device stores licenses from different licensors. Each license can only be created by the licensor as owner. The owner of the hardware or WIBU-SYSTEMS cannot store such a license. No other licensor can store a license of anywhere else. All these restrictions are handled by a mix of symmetric and asymmetric (public key) encryption methods and by private keys.

The stored licenses can be saved by the user as owner of the hardware into a file. All price-relevant information is stored. This information is not encrypted (except some special secret data) but signed individually for each license in dependence of a secret key, delivered by the licensor. The signing is done by a hash via the data which is encrypted by that secret key and stored in the file. The signature is also influenced by the Serial Number of the hardware device (which is unique) and by the current time (second based, hardware device internal), so that no time manipulation is possible.

The user can do this backup as frequently as he or she desires or how frequently it is required (for example after the counting information for pay-per-use is reduced).

This backup file is not required until the hardware device is lost or broken. Then the user buys a new (typically empty) hardware device, which should receive and store all licenses (which must support restoring) from the broken hardware device.

Then a software application outside of the (now unusable) hardware device sends the backup file as a sequence to the Hub Web Service by a single command form the user ("single click"). This central Web Service knows the Restoring Web Services of all licensors who supports such a restore operation. The Hub Web Service analyses the received sequence and sends each license, which supports the restoring, to the corresponding Restoring Web Service. These create new sequences, compatible to the backup sequences, which are sent to the new hardware device. That's why this device receives the new sequences from different Restoring Web Services.

2.2 Avoiding Use of "Lost" or "Broken" Devices

To reduce the chance that a lost device can be reused after found again or a broken device can be reused after a repair or the user claims by cheating a lost or broken device which actually works, the *Locking* Mechanism is introduced:

- The Central Web Service sets the Serial Number of the backup file (res. the lost/broken device) into a "black list". This list is available for all Licensors via a special *Box Validation Service*.
- If a Licensor has to send any Remote Activation Sequence to a hardware device, the Serial Number of this device is checked in this Validation Service. If the Serial Number is listed, a Locking Sequence is immediately sent to the hardware device which locks permanently all security operations in this device.

3 Advantages of the Invention against the "State of the Art"

Today hardware devices which contain values (money card, pay-per-use protection hardware) have typically no automatically working backup/restore mechanism. When such device is lost or broken, the user will lost the stored financial value immediately and permanently or the user receives sometimes a customer-service volunteer "restore", which must be executed manually and which is time-wasting. Some systems support automatic-restore mechanism; but they are not working for different licensors with unique security versa-versa. Moreover, a guarantee that a lost-and-found or a broken-and-repair device cannot be used any longer as a second copy of the stored value, is not handled automatically.

So the device of the invention has following advantages:

- Conserving the saved values by transferring from a lost/broken device into a new device.
- Easy request of the restore information of a lost/broken device from different licensors via a single Hub Web Service by a single action ("click") at user's site and transferring this information into the new (replacement) hardware device.
- A safe method to avoid that lost-and found or broken-and-repaired hardware devices can be used unlimited concurrently to the hardware device, which receives the restored information by the *Locking* mechanism.

4 Appendix

4.1 References

[1] CM-Box Backup, CodeMeter Architecture Description, Version 1.00 of 2003-June-10.

4.2 State of Current Version

This document is preliminary. All contents are subject to change if required.

4.3 Contact Address

If you have further questions or comments, please contact:

WIBU-SYSTEMS AG
Website http://www.wibu.com
E-Mail info@wibu.com
Fax +49-721-93172-22
Phone +49-721-93172-0

Involved persons in this invention: Marcellus Buchheit, Oliver Winzenried

WIBU-SYSTEMS AG

CodeMeter Architecture

CM-Box Backup

Marcellus Buchheit

Version 1.00 of 10. June 2003

Confidential (Level II)

Distribution permitted only inside WIBU-SYSTEMS AG, to distributors or to technical partners.
Do not send to customers or any other interested persons!

Contents

Pages in Document: 10

List of Figures

List of Tables

Error! No table of figures entries found.

1 Introduction

[2003-Jun-07/mabu]

CodeMeter stores all licenses into the hardware "CM-Box". That's why this hardware represents a specific value, defined by the sum of the purchase price of all these licenses. If the CM-Box is broken, stolen or lost, this value is lost too. This may be a big loss for the owner of the CM-Box res. owner of these licenses.

As solution, the CM-Box backup mechanism permits to save the contents of the CM-Box to a file on the PC, which can be restored into another CM Box after the original CM-Box is broken or lost.

This backup mechanism is user-friendly but contains the risk of cheating – a user could claim a broken CM-Box, which works still properly and so trying to get illegal copies of the stored licenses. The backup mechanism of the CM-Box implements several features which reduce sporadic cheating and avoid systematic cheating. All basic and extended features are explained in next chapters.

2 Principles of the CM-Box Backup

[2003-Jun-07/mabu]

The following chapter describes the principle work of the CM-Box Backup. The CM-Box Backup can be described by following basics and highlights:

- Backup file created by User
- Restore fully controlled by Licensor, not WIBU-SYSTEMS
- Licensor can decide restore policy
- Licensor sees only own licenses
- Restore process is single-click action for user
- Backup file cannot be manipulated
- *HiddenData* PIO are encrypted
- *SecretData* PIO are no part of backup
- Restrictions for IFI backup
- Broken or lost CM-Boxes can be locked
- Cheating using the backup/restore mechanism is limited
- Platform for general license transfer

All these topics are explained in the subsequent chapters.

2.1 Backup File Created by User

[2003-Jun-10/mabu]

The CM-Box Backup file is always created at User's Site. It is a XML file which can be copied without any restrictions from one PC to another. It contains the Box Information Structure (Serial Number, Serial Key, CM-Box Version etc.), the IFI (restrictions see chapter 2.9, page 7) and the contents of all Firm Items. All these information blocks may be analyzed separately and can also split into several XML files.

The CM-Box Backup may be started manually by the User via the CM *WebAdmin* dialog. It may also be started by the CM-API and automatically within a time interval which may be specified by the User.

The storing of a single Firm Item with all owned Product Items needs typically between 30 ms and 60 ms. So creating a backup of 500 Firm Items in the CM-Box needs about 30 seconds.

The CES (*Central Execution Service*) maintains a list for each CM-Box which defines for each stored Firm Code when the corresponding Firm Item and all its owning Product Items are stored to the Backup File. One or more of the following options are supported:

(1) After any Remote Activation of the Firm Item
(2) After a specific time interval in seconds resolution

(3) When the user presses the Backup button manually in the WebAdmin

The default setting is all three options active; (2) with an interval of 1 day. If the Firm Item is not defined for restoring by the Licensor, then all three options are inactive.

The list is stored in a CM Backup maintenance WBC file in XML format. The User can modify its contents via the Web Admin console or manually by a XML or text editor.

2.2 Restore Fully Controlled by Licensor, not WIBU-SYSTEMS

[2003-Jun-10/mabu]

The restoring of the backup data – the transfer of Licenses from a broken or lost CM-Box into another CM-Box is handled by a sequence of *Adding Firm Items* and *Adding Product Items* Remote Activation operations. For both operations, the Firm Key is required and this is only known by the Licensor which owns the corresponding Firm Code.

That's why it is principally impossible that WIBU-SYSTEMS, a Trader or a specific backup company could manage the restoring operation.

The Restoring Operation is handled automatically by CM-Talk and executed at Licensor's Site by the License Generator. The Restoring is described and controlled by the PAD (*Product Activation Description*).

If a Licensor decides to support a Restoring of its Firm Items, it sets the URL of the corresponding License Generator as 3d substring of the Firm Text of this Firm Item. If this string is empty or not specified, no Restoring is supported for the corresponding Firm Item.

2.3 Licensor can Decide Restore Policy

[2003-Jun-10/mabu]

The Licensor can decide how the Restoring is handled by specific PAD (*Product Activation Description*) settings. Following variants are available:

- Full Restore without restrictions for a Firm Item and all of its Product Items (with the restriction that *SecretData* PIO cannot be restored, see chapter 2.8, page 7).
- The Restore is restricted to the Firm Item and some of the Product Items.
- Within the Product Item, the current value of a Unit Counter is not completely restored.

The last point is useful because the User could send an old Backup with a much higher Unit Counter value than really exists in the broken or lost CM-Box. Therefore the age of Backup – the time difference between the creation of the Backup and the current time may influence the degree of Unit Counter reduction.

For all other types of PIO such a special restoring is not required because their contents cannot be modified without the control of the Licensor (except *UserData* PIO which are not protected).

The degree of Unit Counter reduction can be set by a linear model between two limits:

- The degree of reduction when the Backup is identical with the current time, named as **MaxUnitCounterRestoreDegree** and a time distance when the reduction starts, named as **MaxUnitCounterRestoreTime**.
- The degree of reduction for the maximum permitted time distance between the Backup and the current time, named as **MinUnitCounterRestoreDegree** and **MinUnitCounterRestoreTime**.

If a backup is not older than the *MaxUnitCounterRestoreTime*, the Unit Counter is 100% replaced.

If a backup is older than the *MinUnitCounterRestoreTime*, the Restoring of the *UnitCounter* PIO is done but the Unit Counter value is set to 0.

A Licensor has set following Unit Counter Restore parameters.

- *MaxUnitCounterRestoreDegree* = 80%, *MaxUnitCounterRestoreTime* = 1 day.
- *MinUnitCounterRestoreDegree* = 10% *MinUnitCounterRestoreTime* = 9 days.

Let a Unit Counter with value 1000. Then it is restored to:

- 1000 when the Backup was done today, closed to the current time.
- 800 when the Backup was the backup was yesterday
- 100 when the Backup was done 9 days ago.
- 0 when the Backup was done 10 days ago.
- 713 when the Backup was done 2 days ago.
- 450 when the Backup was done 5 days ago.
- 280 when the Backup was done 7 days ago.
- 188 when the Backup was done 8 days ago.

The algorithm to calculate a degree within the time interval between *MinUnitCounterRestoreTime* and *MaxUnitCounterRestoreTime* is:

$$Degree = MinDegree + (MaxDegree - MinDegree) \cdot \left(1 - \frac{BackupTime - MinTime}{MinTime - MaxTime}\right)$$

As a User-friendly component, the result of the Unit Counter is rounded up to the next integer value.

2.4 Licensor Sees Only Own Licenses

[2003-Jun-10/mabu]

The User has created a single CM-Box Backup file, but this file is not sent to the Licensors completely: Only that part which describes a specific Firm Item with all owning Product Items is transferred by the Web Communicator to the Licensor as input value for the Restore operation.

This method avoids that a Licensor can discover by analyzing the Back up information which other products are licensed by a specific User.

2.5 Restore Process is Single Action for User

[2003-Jun-10/mabu]

If a CM-Box contains licenses from many Licensors, each of that Licensors contains a separate Restore request via CM-Talk and resends the required Remote Activation operations to the new target CM-Box. The User initializes this operation with a single click to the *Backup* button in the Web Admin console; optionally the User can decide that not all licenses of the Backup are restored; possibly if he or she wants to restore Licenses in several CM-Boxes.

The Web Communicator may initiate the Restore requests to many Licensors at same time, so the Restore operation is started parallel which saves in contrast to a sequential sending of requests a lot of time for the User.

2.6 Backup File Cannot Be Manipulated

[2003-Jun-10/mabu]

The Licensor must have the confirmation to the User that the sent Backup sequence of the Firm Items and Product Items is real and not manipulated. This is done by signing the backup data with a hash code using SHA-256 within the CM-Box. The hash code is then AES-encrypted by the secret Firm Key and appended as 16-byte TVB to the Backup information. Because the Firm Key is only known for the Licensor, no manipulation is possible – even WIBU-SYSTEMS could not create a signed Backup sequence of wrong data.

Each Backup sequence for a Firm Item includes also the three time-values of the CM-Box (Certified Box Clock, Running Box Clock and System Box Clock) and the Serial Number. So using a Backup structure of another CM-Box or of another time is not possible.

Moreover the encryption of the hash of the signing does not depends only of the Firm Key but also of the Serial Number, the Firm Update Counter in the Firm Item and the current time in the CM-Box (identical with System Box Clock).

The secret Firm Key is **no** part of the Backup sequence.

A big advantage of a signed and manipulation-free Backup sequence is that there is no requirement for the Licensor to save an own backup of all created licenses. The Licensor can do this and even use such information for a double check; but there is no technical nor security reason to do that.

2.7 HiddenData PIO is Encrypted

[2003-Jun-10/mabu]

Typically all data in a backup structure are readable. This information is not secret and simplifies the analyses of the backup structure.

One exception is a *HiddenData* PIO: In contrast to a *SecretData* PIO, they can be part of the backup; but in contrast to all other PIO, the information is encrypted by AES-CBC. The used key is identical with that which is used to encrypt the hash of the signing (see chapter 2.6, page 6) and depends on the Firm Key, Firm Code, Firm Update Counter, Serial Number and time when the backup was created.

2.8 SecretData PIO is No Part of Backup

[2003-Jun-10/mabu]

In contrast to all other PIO, a *SecretData* PIO cannot be part of a backup. Such data may be created randomly within the CM-Box and should be always secret outside of the CM-Box, even for the Licensor who creates the Product Item which contains the *SecretData* PIO.

The PAD (*Product Activation Description*) at Licensor's Site permits two options to restore a *SecretData* PIO:

- The PIO is *not* restored
- The PIO is restored with fixed data, random data or a combination of both.

2.9 Restrictions of IFI Backup

[2003-Jun-10/mabu]

The User can do an own Backup of its IFI (Implicit Firm Item). A local application (not available in the moment) can restore the User-orientated UPI (User Product Item) and all Product Items with a higher Product Code than that of the UPI into another CM-Box. Instead of the Firm Key of a normal license, the User Key is responsible for signing the data hash and encrypting the *HiddenData* PIO.

A security risk for the User is the encryption of *HiddenData* PIO in a UPI if the User Key is not the UIK (*User Individual Key*) but the UCK (*User Common Key*): The UCK Key is available for WIBU-SYSTEMS and also used during the Locking operation (chapter 2.10 page 7). So it would be principally possibly for WIBU-SYSTEMS or for a Licensor (after receiving the UCK for Locking) to decrypt the *HiddenData* PIO in the IFI backup.

To avoid this risk, a Backup sequence of the IFI (*Implicit Firm Item*) can only be done if the User Key is the UIK (*User Individual Key*); the creation of the IFI Backup sequence in the CM-Box fails if the UCK (*User Common Key*) is stored as User Key.

2.10 Broken or Lost CM-Boxes can be Locked

[2003-Jun-10/mabu]

The CM-Box Backup and Restore mechanism is friendly for the User but could also be used for manipulation:

- A User creates a valid Backup Sequence of a CM-BOX "A".

- The User claims that the CM-Box "A" is broken or lost but this is wrong.
- The Licensor creates a Restore of its License from the Backup Sequence into a new CM-Box "B".

The User can now use two licenses: That in CM-Box "A" and that in CM-Box "B".

There is no chance to avoid this: Because an important feature of CodeMeter is the offline-use of a CM-Box, no Online-checking is possible to check that CM-Box "A" is really lost or broken.

The same risk is when a CM-Box is stolen – the owner receives a restore into another CM-Box, but the thief can also use the licenses in the stolen CM-Box.

The first chance to detect a broken CM-Box which is not broken or a stolen CM-Box at the Thief's Site is any online activity. CodeMeter requires such online activity for Remote Activation via CM-Talk and for setting the CTS (*Certified Time Stamp*).

As solution, CodeMeter supports a Locking mechanism to lock a broken or lost CM-Box when it is detected within the Internet during Remote Activation or Certified Time Stamp. Following mechanism is used:

- If a Licensor creates a Restore, it sets the signed Serial Number of the Backup Sequence into a local Locking List.
- When the User specifies a CM-Box with the same Serial Number again for Remote Activation, the Licensor detects this CM-Box as broken or lost and rejects the Remote Activation. This is a local activity which is independent of the centralized locking management by WIBU-SYSTEMS.
- As a second operation, the Licensor sends the Serial Number of the CM-Box, for which the Backup Sequence was created, to WIBU-SYSTEMS or an affiliated partner for CM-Box Locking Management. This CM-Box is a candidate for lost, broken or stolen.
- This Locking instance checks whether the Request for Locking came from an authorized Licensor. If so, it is checked if the CM-Box with this Serial Number is already locked.
- If the CM-Box is not locked, a Locking Sequence is created and set into a database which can be read by authorized Licensors and Certified Time Server Partners.
- Each Licensor or Certified Time Server Partner download this list of locked CM-Box – all of these CM-Boxes are declared as broken, stolen or lost by the User as original Owner.
- If a Licensor receives now a request for Remote Activation or a Certified Time Server Partner a request for a Certified Time Stamp, it searches the Serial Number of the target CM-Box in the Locking list.
- If the target CM-Box is not detected as locked, the operation continues as usual. But if the target CM-Box is detected as locked, the Licensor or the Certified Time Server partner sends the created Locking Sequence to the User, the Web Communicator interprets this command, sends it to the CM-Box and this is locked – it cannot longer be used for any encryption or authentication, even the most PIO data cannot be longer read.

Sometimes it may be that the Locking fails: A hacker could be a Licensor of WIBU-SYSTEMS and tries to lock all CM-Boxes in the field from which he or she has received a Backup Sequence. CodeMeter reduces the limit of such a criminal act by two features

- The source of such wrong locking requests can be found by authentication of the Licensor and eliminated.
- WIBU-SYSTEMS can also unlock a previously locked CM-Box. This is an operation which is handled exclusively by WIBU-SYSTEMS; it is not planned that a Licensor can do this too.

2.11 Cheating Using Backup/Restore Mechanism is Limited

[2003-Jun-10/mabu]

If a User knows about the details of CM Box Locking, he or she could avoid any online use with the CM-Box which was claimed as broken, lost or stolen. He or she could buy many CM-Boxes and try to repeat the Backup/Restore mechanism from one CM-Box to the next one to receive a lot of licenses and try to sell them.

Such a criminal act can be avoided if a Licensor stores a list of Serial Numbers which are a target of a Restore Operation. If such a CM-Box is claimed as broken, lost or stolen after a short time interval and it is asked for

a Restore into another CM-Box, the Licensor is alarmed and can stop the automatic repeated Restore-Process until evidences are available about the owner of this CM-Box, its using practice etc.

The *Repeated Restoring Alert List* is managed by the PAD Programmer at Licensor's Site. The Licensor can specify two parameters:

- The number of maximum Restore Operations via a chain of CM Boxes within a time interval to send an alert.
- The number of maximum Restore Operations via a chain of CM Boxes within a time interval to stop the Restore operation automatically.

2.12 Platform for License Transfer

[2003-Jun-10/mabu]

The Backup/Restore mechanism can also be used to transfer a License from CM-Box to another. The difference between a Transfer and a Restore is that for a Transfer the CM-Box which was the original location of the License is not broken, lost or stolen and is no candidate for Locking (see chapter 2.10, page 7).

The License Transfer is very similar to the Backup with the difference that the Firm Item is deleted completely in the CM-Box of the previous location before the Backup is executed. A big advantage is that the Licensor may not backup the License during the Transfer because this is the responsibility of the User.

Such a Transfer is executed in following steps:

- The User wants that a License is transfer from one CM-Box "A" to another CM-Box "B".
- The User creates a Backup Sequence of CM-Box "A".
- The User sends the Transfer Request to the Licensor (similar to a Backup Request), specifying the Backup Sequence of CM-Box "A" and the CM-Box "B" information (Serial Number etc.)
- The Licensors sends a "Delete Firm Item" command the CM-Box "A" and deletes the license there completely.
- The Licensor sends a Restore Sequence to the CM-Box "B".

If any operation fails, the User can resend the information that the Firm Item is deleted in the CM-Box "A", the backup of the contents and the License Transfer can be completed again by the Licensor.

Note

A *SecretData* PIO cannot be transferred because this is a principle restriction of the CM-Box Backup/Restore operations by security reason (see chapter 2.8, page 7).

3 The Contents of a Backup File

[2003-Jun-10/mabu]

[TBA]

4 Implementation at User's Site

[2003-Jun-10/mabu]

[TBA]

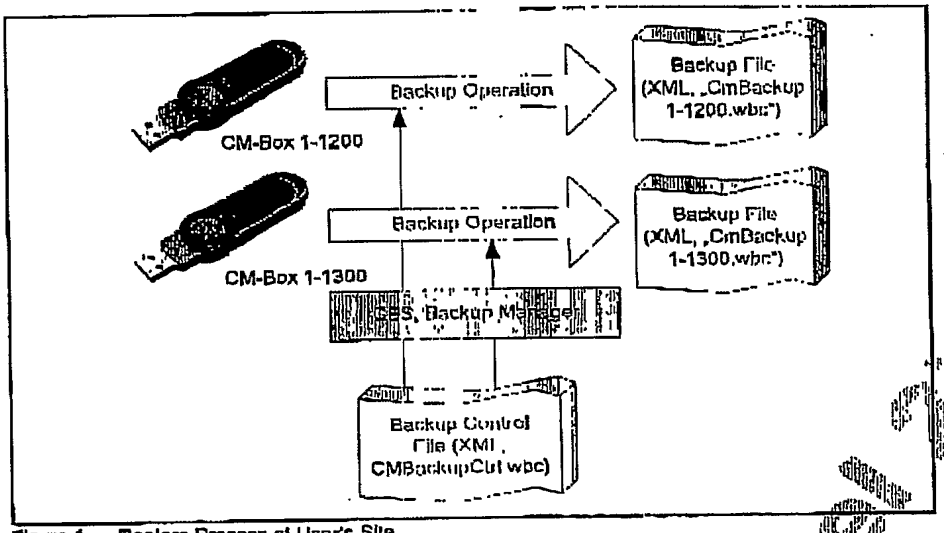

Figure 1 Restore Process at User's Site

[TBA]

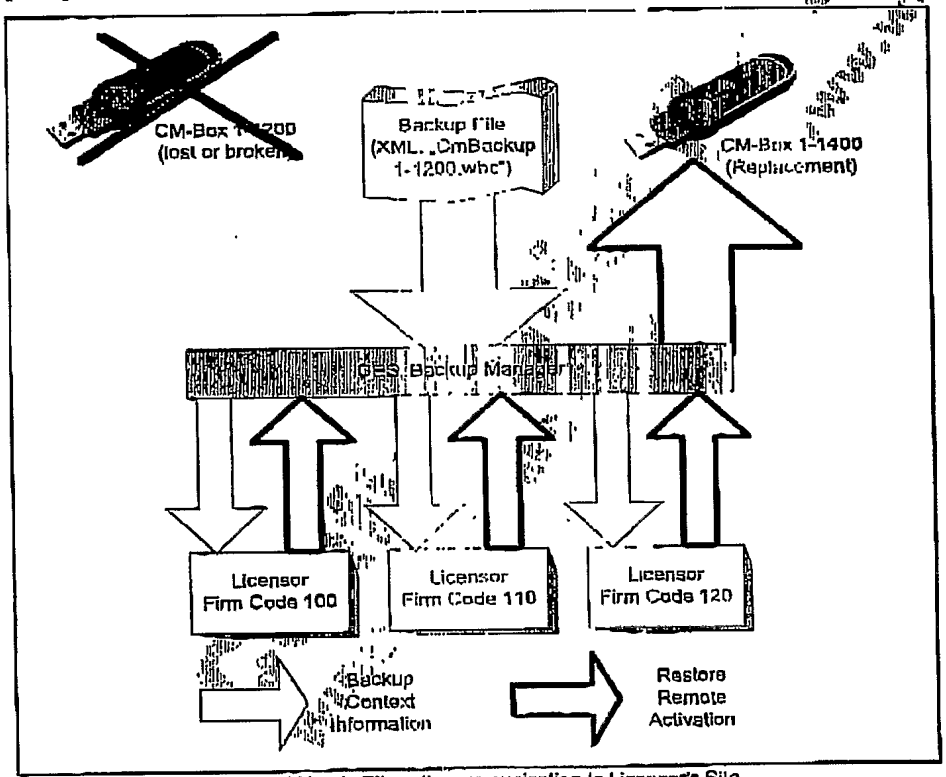

Figure 2 Resore Process at User's Site with communication to Licensor's Site

[TBA]

5 Implementation at Licensor's Site

[2003-Jun-10/mabu]

[TBA]

6 The Locking Infrastructure

[2003-Jun-10/mabu]

[TBA]

7 Appendices

7.1 State of Current Version

This document describes implemented technology but it is under discussion.

7.2 Contact Address

If you have further questions or comments, please contact:

WIBU-SYSTEMS AG
Website http://www.wibu.com
E-Mail info@wibu.com
Fax +49-721-93172-22
Phone +49-721-93172-0

W 5839/03-EU

Patent Claim

A method to restore data, which is stored in a broken computer hardware device by transferring them partially or completely into another hardware device of same type, the method including a complete backup mechanism, characterized by the following steps:

The hardware device stores licenses from different licensors. Each license can only be created by the licensor as owner. The owner of the hardware or WIBU-SYSTEMS cannot store such a license. No other licensor can store a license of anywhere else. All these restrictions are handled by a mix of symmetric and asymmetric (public key) encryption methods and by private keys.

The stored licenses can be saved by the user as owner of the hardware into a file. All price-relevant information is stored. This information is not encrypted (except some special secret data) but signed individually for each license in dependence of a secret key, delivered by the licensor. The signing is done by a hash via the data which is encrypted by that secret key and stored in the file. The signature is also influenced by the Serial Number of the hardware device (which is unique) and by the current time (second based, hardware device internal), so that no time manipulation is possible.

The user can do this backup as frequently as he or she desires or how frequently it is required (for example after the counting information for pay-per-use is reduced).

This backup file is not required until the hardware device is lost or broken. Then the user buys a new (typically empty) hardware device, which should receive and store all licenses (which must support restoring) from the broken hardware device.

Then a software application outside of the (now unusable) hardware device sends the backup file as a sequence to the Hub Web Service by a single command form the user ("single click"). This central Web Service knows the Restoring Web Services of all licensors who supports such a restore operation. The Hub Web Service analyses the received sequence and sends each license, which supports the restoring, to the corresponding Restoring Web Service. These create new sequences, compatible to the backup sequences, which are sent to the new hardware device. That's why this device receives the new sequences from different Restoring Web Services.